# Chapter 1

# Coding theory and algebraic combinatorics

Michael Huber*

*Institut für Mathematik, Technische Universität Berlin,
Straße des 17. Juni 136, D-10623 Berlin, Germany,
mhuber@math.tu-berlin.de*

This chapter introduces and elaborates on the fruitful interplay of coding theory and algebraic combinatorics, with most of the focus on the interaction of codes with combinatorial designs, finite geometries, simple groups, sphere packings, kissing numbers, lattices, and association schemes. In particular, special interest is devoted to the relationship between codes and combinatorial designs. We describe and recapitulate important results in the development of the state of the art. In addition, we give illustrative examples and constructions, and highlight recent advances. Finally, we provide a collection of significant open problems and challenges concerning future research.

## 1.1. Introduction

The classical publications "A mathematical theory of communication" by C. E. Shannon [1] and "Error detecting and error correcting codes" by R. W. Hamming [2] gave birth to the twin disciplines of information theory and coding theory. Since their inceptions the interactions of information and coding theory with many mathematical branches have continually deepened. This is in particular true for the close connection between coding theory and algebraic combinatorics.

This chapter introduces and elaborates on this fruitful interplay of coding theory and algebraic combinatorics, with most of the focus on the interaction of codes with combinatorial designs, finite geometries, simple groups, sphere packings, kissing numbers, lattices, and association schemes. In particular, special interest is devoted to the relationship between codes and combinatorial designs. Since we do not assume the reader is familiar with the theory of combinatorial designs, an accessible and reasonably self-contained exposition is provided. Subsequently, we describe and recapitulate important results in the development of the state of the art, provide illustrative examples and constructions, and highlight recent advances. Furthermore, we give a collection of significant open problems and challenges concerning future research.

The chapter is organized as follows. In Sec. 1.2, we give a brief account of basic notions of algebraic coding theory. Section 1.3 consists of the main part of the chapter: After an introduction to finite projective planes and combinatorial designs, a subsection on basic connections between codes and combinatorial designs follows. The next subsection is on perfect codes and designs, and addresses further related concepts. Subsection 1.3.4 deals with the classical Assmus-Mattson Theorem and various analogues. A subsection on codes and finite geometries follows the discussion on the non-existence of a projective plane of order 10. In Subsection 1.3.6, interrelations between the Golay codes, the Mathieu-Witt designs, and the Mathieu groups are studied. Subsection 1.3.7 deals with the Golay codes and the Leech lattice, as well as recent milestones concerning kissing numbers and sphere packings. The last topic of this section considers codes and association schemes. The chapter concludes with sections on directions for further research as well as conclusions and exercises.

## 1.2.  Background

For our further purposes, we give a short account of basic notions of algebraic coding theory. For additional information on the subject of algebraic coding theory, the reader is referred to [3–13]. For some historical notes on its origins, see [14] and [6, Chap. 1], as well as [15] for a historical survey on coding theory and information theory.

We denote by $\mathbb{F}^n$ the set of all $n$-tuples from a $q$-symbol alphabet. If $q$ is a prime power, we take the finite field $\mathbb{F} = \mathbb{F}_q$ with $q$ elements, and interpret $\mathbb{F}^n$ as an $n$-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. The elements of $\mathbb{F}^n$ are called *vectors* (or *words*) and will be denoted by bold symbols.

The *(Hamming) distance* between two codewords $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ is defined by the number of coordinate positions in which they differ, i.e.

$$d(\mathbf{x}, \mathbf{y}) := |\{i \mid 1 \leq i \leq n, \ x_i \neq y_i\}| \,.$$

The *weight* $w(\mathbf{x})$ of a codeword $\mathbf{x}$ is defined by

$$w(\mathbf{x}) := d(\mathbf{x}, \mathbf{0}),$$

whenever 0 is an element of $\mathbb{F}$.

A subset $C \subseteq \mathbb{F}^n$ is called a *(q-ary) code* of *length $n$* (*binary* if $q = 2$, *ternary* if $q = 3$). The elements of $C$ are called *codewords*. A *linear code* (or *$[n, k]$ code*) over the field $\mathbb{F}_q$ is a $k$-dimensional linear subspace $C$ of the vector space $\mathbb{F}_q^n$. We note that large parts of coding theory are concerned with linear codes. In particular, as many combinatorial configurations can be described by their incidence matrices, coding theorists have started in the early 1960's to consider as codes the vector spaces spanned by the rows of the respective incidence matrices over some given field.

The *minimum distance* $d$ of a code $C$ is defined as

$$d := \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \ \mathbf{x} \neq \mathbf{y}\}.$$

Clearly, the minimum distance of a linear code is equal to its *minimum weight*, i.e. the minimum of the weights of all non-zero codewords. An $[n, k, d]$ code is an $[n, k]$ code with minimum distance $d$.

The minimum distance of a (not necessarily linear) code $C$ determines the error-correcting capability of $C$: If $d = 2e + 1$, then $C$ is called an *e-error-correcting code*. Defining by

$$S_e(\mathbf{x}) := \{\mathbf{y} \in \mathbb{F}^n \mid d(\mathbf{x}, \mathbf{y}) \leq e\}$$

the *sphere* (or *ball*) of radius $e$ around a codeword $\mathbf{x}$ of $C$, this implies that the spheres of radius $e$ around distinct codewords are disjoint.

Counting the number of codewords in a sphere of radius $e$ yields to the subsequent *sphere packing* (or *Hamming*) *Bound*.

**Theorem 1.1.** *Let $C$ be a $q$-ary code of length $n$ and minimum distance $d = 2e + 1$. Then*

$$|C| \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i \leq q^n.$$

If equality holds, then $C$ is called a *perfect code*. Equivalently, $C$ is perfect if the spheres of radius $e$ around all codewords cover the whole space $\mathbb{F}^n$. Certainly, perfect codes are combinatorially interesting objects, however, they are extremely rare.

We will call two codes *(permutation) equivalent* if one is obtained from the other by applying a fixed permutation to the coordinate positions for all codewords. A *generator matrix* $G$ for an $[n, k]$ code $C$ is a $(k \times n)$-matrix for which the rows are a basis of $C$. We say that $G$ is in *standard form* if $G = (I_k, P)$, where $I_k$ is the $(k \times k)$ identity matrix.

For an $[n, k]$ code $C$, let

$$C^\perp := \{\mathbf{x} \in \mathbb{F}_q^n \mid \forall_{\mathbf{y} \in C}[\langle \mathbf{x}, \mathbf{y} \rangle = 0]\}$$

denote the *dual code* of $C$, where $\langle \mathbf{x}, \mathbf{y} \rangle$ is the standard inner (or dot) product in $\mathbb{F}_q^n$. The code $C^\perp$ is an $[n, n - k]$ code. If $H$ is a generator matrix for $C^\perp$, then clearly

$$C = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x} H^T = \mathbf{0}\},$$

and $H$ is called a *parity check matrix* for the code $C$. If $G = (I_k, P)$ is a generator matrix of $C$, then $H = (-P^T, I_{n-k})$ is a parity check matrix of $C$. A code $C$ is called *self-dual* if $C = C^\perp$. If $C \subset C^\perp$, then $C$ is called *self-orthogonal*.

If $C$ is a linear code of length $n$ over $\mathbb{F}_q$, then

$$\overline{C} := \{(c_1, \ldots, c_n, c_{n+1}) \mid (c_1, \ldots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}$$

defines the *extended code* corresponding to $C$. The symbol $c_{n+1}$ is called the *overall parity check symbol*. Conversely, $C$ is the *punctured* (or *shortened*) code of $\overline{C}$.

The *weight distribution* of a linear code $C$ of length $n$ is the sequence $\{A_i\}_{i=0}^n$, where $A_i$ denotes the number of codewords in $C$ of weight $i$. The polynomial

$$A(x) := \sum_{i=0}^{n} A_i x^i$$

is the *weight enumerator* of $C$.

The weight enumerators of a liner code and its dual code are related, as shown by the following theorem, which is one of the most important results in the theory of error-correcting codes.

**Theorem 1.2.** (MacWilliams [16]). *Let $C$ be an $[n, k]$ code over $\mathbb{F}_q$ with weight enumerator $A(x)$ and let $A^\perp(x)$ be the weight enumerator of the dual code $C^\perp$. Then*

$$A^\perp(x) = q^{-k}(1 + (q-1)x)^n A\big(\frac{1-x}{1+(q-1)x}\big).$$

We note that the concept of the weight enumerator can be generalized to non-linear codes (so-called *distance enumerator*, cf. [17, 18] and Subsection 1.3.8).

An $[n, k]$ code $C$ over $\mathbb{F}_q$ is called *cyclic* if

$$\forall_{(c_0, c_1, \ldots, c_{n-1}) \in C}[(c_{n-1}, c_0, \ldots, c_{n-2}) \in C],$$

i.e. any cyclic shift of a codeword is again a codeword. We adopt the usual convention for cyclic codes that $n$ and $q$ are coprime. Using the isomorphism

$$(a_0, a_1, \ldots, a_{n-1}) \rightleftarrows a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$$

between $\mathbb{F}_q^n$ and the residue class ring $\mathbb{F}_q[x]/(x^n - 1)$, it follows that a cyclic code corresponds to an ideal in $\mathbb{F}_q[x]/(x^n - 1)$.

## 1.3. Thoughts for Practitioners

In the following, we introduce and elaborate on the fruitful interplay of coding theory and algebraic combinatorics, with most of the focus on the interaction of codes with combinatorial designs, finite geometries, simple groups, sphere packings, kissing numbers, lattices, and association schemes. In particular, special interest is devoted to the relationship between codes and combinatorial designs. We give an accessible and reasonably self-contained exposition in the first subsection as we do not assume the reader is familiar with the theory of combinatorial designs. In what

follows, we describe and recapitulate important results in the development of the state of the art. In addition, we give illustrative examples and constructions, and highlight recent achievements.

### 1.3.1. *Introduction to finite projective planes and combinatorial designs*

Combinatorial design theory is a subject of considerable interest in discrete mathematics. We give in this subsection an introduction to the topic, with emphasis on the construction of some important designs. For a more general treatment of combinatorial designs, the reader is referred to [19–24]. In particular, [19, 21] provide encyclopedias on key results.

Besides coding theory, there are many interesting connections of design theory to other fields. We mention in our context especially its links to finite geometries [25], incidence geometry [26], group theory [27–30], graph theory [4, 31], cryptography [32–34], as well as classification algorithms [35]. In addition to that, we recommend [22, 36–39] for the reader interested in the broad area of combinatorics in general.

We start by introducing several notions.

**Definition 1.1.** A *projective plane of order* $n$ is a pair of *points* and *lines* such that the following properties hold:

 (i) any two distinct points are on a unique line,
 (ii) any two distinct lines intersect in a unique point,
(iii) there exists a *quadrangle*, i.e. four points no three of which are on a common line,
(iv) there are $n + 1$ points on each line, $n + 1$ lines through each point and the total number of points, respectively lines, is $n^2 + n + 1$.

It follows easily from (i), (ii), and (iii) that the number of points on a line is a constant. When setting this constant equal to $n + 1$, then (iv) is a consequence of (i) and (iii).

Combinatorial designs can be regarded as generalizations of projective planes:

**Definition 1.2.** For positive integers $t \leq k \leq v$ and $\lambda$, we define a *t-design*, or more precisely a *t-$(v, k, \lambda)$ design*, to be a pair $\mathcal{D} = (X, \mathcal{B})$, where $X$ is a finite set of *points*, and $\mathcal{B}$ a set of $k$-element subsets of $X$ called *blocks*, with the property that any $t$ points are contained in precisely $\lambda$ blocks.

We will denote points by lower-case and blocks by upper-case Latin letters. Via convention, we set $v := |X|$ and $b := |\mathcal{B}|$. Throughout this chapter, 'repeated blocks' are not allowed, that is, the same $k$-element subset of points may not occur twice as a block. If $t < k < v$ holds, then we speak of a *non-trivial* $t$-design.

Designs may be represented algebraically in terms of incidence matrices: Let $\mathcal{D} = (X, \mathcal{B})$ be a $t$-design, and let the points be labeled $\{x_1, \ldots, x_v\}$ and the blocks be labeled $\{B_1, \ldots, B_b\}$. Then, the $(b \times v)$-matrix $A = (a_{ij})$ $(1 \le i \le b, 1 \le j \le v)$ defined by

$$a_{ij} := \begin{cases} 1, \text{ if } x_j \in B_i \\ 0, \text{ otherwise} \end{cases}$$

is called an *incidence matrix* of $\mathcal{D}$. Clearly, $A$ depends on the respective labeling, however, it is unique up to column and row permutation.

If $\mathcal{D}_1 = (X_1, \mathcal{B}_1)$ and $\mathcal{D}_2 = (X_2, \mathcal{B}_2)$ are two $t$-designs, then a bijective map $\alpha : X_1 \longrightarrow X_2$ is called an *isomorphism* of $\mathcal{D}_1$ onto $\mathcal{D}_2$, if

$$B \in \mathcal{B}_1 \iff \alpha(B) \in \mathcal{B}_2.$$

In this case, the designs $\mathcal{D}_1$ and $\mathcal{D}_2$ are *isomorphic*. An isomorphism of a design $\mathcal{D}$ onto itself is called an *automorphism* of $\mathcal{D}$. Evidently, the set of all automorphisms of a design $\mathcal{D}$ form a group under composition, the *full automorphism group* of $\mathcal{D}$. Any subgroup of it will be called *an automorphism group* of $\mathcal{D}$.

If $\mathcal{D} = (X, \mathcal{B})$ is a $t$-$(v, k, \lambda)$ design with $t \ge 2$, and $x \in X$ arbitrary, then the *derived design with respect to* $x$ is $\mathcal{D}_x = (X_x, \mathcal{B}_x)$, where $X_x = X \backslash \{x\}$, $\mathcal{B}_x = \{B \backslash \{x\} \mid x \in B \in \mathcal{B}\}$. In this case, $\mathcal{D}$ is also called an *extension* of $\mathcal{D}_x$. Obviously, $\mathcal{D}_x$ is a $(t-1)$-$(v-1, k-1, \lambda)$ design. The *complementary design* $\overline{\mathcal{D}}$ is obtained by replacing each block of $\mathcal{D}$ by its complement.

For historical reasons, a $t$-$(v, k, \lambda)$ design with $\lambda = 1$ is called a *Steiner $t$-design*. Sometimes this is also known as a *Steiner system* if the parameter $t$ is clearly given from the context.

The special case of a Steiner design with parameters $t = 2$ and $k = 3$ is called a *Steiner triple system of order* $v$ (briefly $STS(v)$). The question regarding their existence was posed in the classical "Combinatorische Aufgabe" (1853) of the nineteenth century geometer Jakob Steiner [40]:

> "Welche Zahl, $N$, von Elementen hat die Eigenschaft, dass sich die Elemente so zu dreien ordnen lassen, dass je zwei in einer, aber nur in einer Verbindung vorkommen?"

However, there had been earlier work on these particular designs going back to, in particular, J. Plücker, W. S. B. Woolhouse, and most notably T. P. Kirkman. For an account on the early history of designs, see [21, Chap. I.2] and [41].

A Steiner design with parameters $t = 3$ and $k = 4$ is called a *Steiner quadruple system of order* $v$ (briefly $SQS(v)$).

If a 2-design has equally many points and blocks, i.e. $v = b$, then we speak of a *square design* (as its incidence matrix is square). By tradition, square designs are often called *symmetric designs*, although here the term does not imply any symmetry of the design. For more on these interesting designs, see, e.g., [42].

We give some illustrative examples of finite projective planes and combinatorial designs. We assume that $q$ is always a prime power.

**Example 1.1.** Let us choose as point set

$$X = \{1, 2, 3, 4, 5, 6, 7\}$$

and as block set

$$\mathcal{B} = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{1, 5, 6\}, \{2, 6, 7\}, \{1, 3, 7\}\}.$$

This gives a 2-$(7, 3, 1)$ design, the well-known *Fano plane*, the smallest design arising from a projective geometry, which is unique up to isomorphism. We give the usual representation of this projective plane of order 2 by the following diagram:
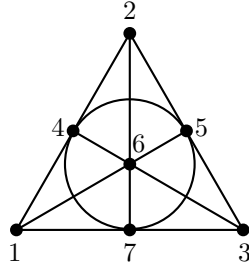


Fig. 1.1.   Fano plane

**Example 1.2.** We take as point set

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

and as block set

$$\mathcal{B} = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\},$$

$$\{1, 5, 9\}, \{2, 6, 7\}, \{3, 4, 8\}, \{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}\}.$$

This gives a 2-$(9, 3, 1)$ design, the smallest non-trivial design arising from an affine geometry, which is again unique up to isomorphism. This affine plane of order 3 can be constructed from the array

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array}$$
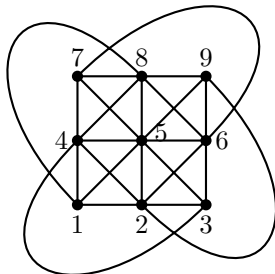
as shown in Figure 1.2.

Fig. 1.2.   Affine plane of order 3

More generally, we obtain:

**Example 1.3.**  We choose as point set $X$ the set of 1-dimensional subspaces of a vector space $V = V(d,q)$ of dimension $d \geq 3$ over $\mathbb{F}_q$. As block set $\mathcal{B}$ we take the set of 2-dimensional subspaces of $V$. Then there are $v = (q^d - 1)/(q - 1)$ points and each block $B \in \mathcal{B}$ contains $k = q + 1$ points. Since obviously any two 1-dimensional subspaces span a single 2-dimensional subspace, any two distinct points are contained in a unique block. Thus, the *projective space* $PG(d - 1, q)$ is an example of a 2-$(\frac{q^d-1}{q-1}, q + 1, 1)$ design. For $d = 3$, the particular designs are *projective planes of order* $q$, which are square designs. More generally, for any fixed $i$ with $1 \leq i \leq d - 2$, the points and $i$-dimensional subspaces of $PG(d - 1, q)$ (i.e. the $(i + 1)$-dimensional subspaces of $V$) yield a 2-design.

**Example 1.4.**  We take as point set $X$ the set of elements of a vector space $V = V(d,q)$ of dimension $d \geq 2$ over $\mathbb{F}_q$. As block set $\mathcal{B}$ we choose the set of affine lines of $V$ (i.e. the translates of 1-dimensional subspaces of $V$). Then there are $v = q^d$ points and each block $B \in \mathcal{B}$ contains $k = q$ points. As clearly any two distinct points lie on exactly one line, they are contained in a unique block. Hence, we obtain the *affine space* $AG(d,q)$ as an example of a 2-$(q^d, q, 1)$ design. When $d = 2$, these designs are *affine planes of order* $q$. More generally, for any fixed $i$ with $1 \leq i \leq d - 1$, the points and $i$-dimensional subspaces of $AG(d,q)$ form a 2-design.

**Remark 1.1.** It is well-established that both affine and projective planes of order $n$ exist whenever $n$ is a prime power. The conjecture that no such planes exist with orders other than prime powers is unresolved so far. The classical result of R. H. Bruck and H. J. Ryser [43] still remains the only general statement: If $n \equiv 1$ or 2 (mod 4) and $n$ is not equal to the sum of two squares of integers, then $n$ does not occur as the order of a finite projective plane. The smallest integer that is not a prime power and not covered by the Bruck-Ryser Theorem is 10. Using substantial

computer analysis, C. W. H. Lam, L. Thiel, and S. Swiercz [44] proved the non-existence of a projective plane of order 10 (cf. Remark 1.10). The next smallest number to consider is 12, for which neither a positive nor a negative answer has been proved.

Needless to mention that — apart from the existence problem — the question on the number of different isomorphism types (when existent) is fundamental. There are, for example, precisely four non-isomorphic projective planes of order 9. For a further discussion, in particular of the rich history of affine and projective planes, we refer, e.g., to [25, 45–49].

**Example 1.5.** We take as points the vertices of a 3-dimensional cube. As illustrated in Figure 1.3, we can choose three types of blocks:

 (i)  a face (six of these),
(ii)  two opposite edges (six of these),
(iii)  an inscribed regular tetrahedron (two of these).

This gives a 3-$(8, 4, 1)$ design, which is unique up to isomorphism.
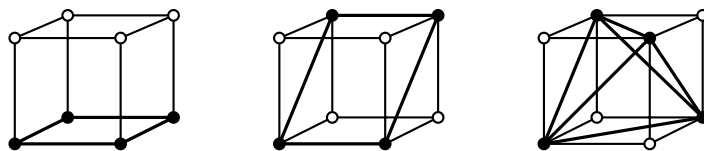


Fig. 1.3.   Steiner quadruple system of order 8

We have more generally:

**Example 1.6.** In $AG(d, q)$ any three distinct points define a plane unless they are collinear (that is, lie on the same line). If the underlying field is $\mathbb{F}_2$, then the lines contain only two points and hence any three points cannot be collinear. Therefore, the points and planes of the affine space $AG(d, 2)$ form a 3-$(2^d, 4, 1)$ design. More generally, for any fixed $i$ with $2 \leq i \leq d-1$, the points and $i$-dimensional subspaces of $AG(d, 2)$ form a 3-design.

**Example 1.7.**   The unique 2-$(9, 3, 1)$ design whose points and blocks are the points and lines of the affine plane $AG(2, 3)$ can be extended precisely three times to the following designs which are also unique up to isomorphism: the 3-$(10, 4, 1)$ design which is the Möbius plane of order 3 with $P\varGamma L(2, 9)$ as full automorphism group, and the two *Mathieu-Witt designs* 4-$(11, 5, 1)$ and 5-$(12, 6, 1)$ with the sporadic Mathieu groups $M_{11}$ and $M_{12}$ as point 4-transitive and point 5-transitive full automorphism groups, respectively.

To construct the 'large' Mathieu-Witt designs one starts with the $2$-$(21, 5, 1)$ design whose points and blocks are the points and lines of the projective plane $PG(2, 4)$. This can be extended also exactly three times to the following unique designs: the *Mathieu-Witt design* $3$-$(22, 6, 1)$ with $\mathrm{Aut}(M_{22})$ as point 3-transitive full automorphism group as well as the *Mathieu-Witt designs* $4$-$(23, 7, 1)$ and $5$-$(24, 8, 1)$ with $M_{23}$ and $M_{24}$ as point 4-transitive and point 5-transitive full automorphism groups, respectively.

The five Mathieu groups were the first sporadic simple groups and were discovered by E. Mathieu [50, 51] over one hundred years ago. They are the only finite 4- and 5-transitive permutation groups apart from the symmetric or alternating groups. The Steiner designs associated with the Mathieu groups were first constructed by both R. D. Carmichael [28] and E. Witt [52], and their uniqueness established up to isomorphism by Witt [53]. From the meanwhile various alternative constructions, we mention especially those of H. Lüneburg [54] and M. Aschbacher [55, Chap. 6]. However, the easiest way to construct and prove uniqueness of the Mathieu-Witt designs is via coding theory, using the related *binary* and *ternary Golay codes* (see Subsection 1.3.6).

**Remark 1.2.** By classifying Steiner designs which admit automorphism groups with sufficiently strong symmetry properties, specific characterizations of the Mathieu-Witt designs with their related Mathieu groups were obtained (see, e.g., [56–61] and [62, Chap. 5] for a survey).

**Remark 1.3.** We mention that, in general, for $t = 2$ and 3, there are many infinite classes of Steiner $t$-designs, but for $t = 4$ and 5 only a finite number are known. Although L. Teirlinck [63] has shown that non-trivial $t$-designs exist for all values of $t$, no Steiner $t$-designs have been constructed for $t \geq 6$ so far.

In what follows, we need some helpful combinatorial tools:

A standard combinatorial double counting argument gives the following assertions.

**Lemma 1.1.** *Let* $\mathcal{D} = (X, \mathcal{B})$ *be a* $t$-$(v, k, \lambda)$ *design. For a positive integer* $s \leq t$, *let* $S \subseteq X$ *with* $|S| = s$. *Then the total number* $\lambda_s$ *of blocks containing all the points of* $S$ *is given by*

$$\lambda_s = \lambda \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

*In particular, for* $t \geq 2$, *a* $t$-$(v, k, \lambda)$ *design is also an* $s$-$(v, k, \lambda_s)$ *design.*

For historical reasons, it is customary to set $r := \lambda_1$ to be the total number of blocks containing a given point (referring to the 'replication number' from statistical design of experiments, one of the origins of designs theory).

**Lemma 1.2.** *Let $\mathcal{D} = (X, \mathcal{B})$ be a $t$-$(v, k, \lambda)$ design. Then the following holds:*

(a) $bk = vr$.

(b) $\binom{v}{t}\lambda = b\binom{k}{t}$.

(c) $r(k-1) = \lambda_2(v-1)$ *for $t \geq 2$.*

Since in Lemma 1.1 each $\lambda_s$ must be an integer, we have moreover the subsequent necessary arithmetic conditions.

**Lemma 1.3.** *Let $\mathcal{D} = (X, \mathcal{B})$ be a $t$-$(v, k, \lambda)$ design. Then*

$$\lambda\binom{v-s}{t-s} \equiv 0 \,(\mathrm{mod}\,\binom{k-s}{t-s}))$$

*for each positive integer $s \leq t$.*

The following theorem is an important result in the theory of designs, generally known as *Fisher's Inequality*.

**Theorem 1.3.** (Fisher [64]). *If $\mathcal{D} = (X, \mathcal{B})$ is a non-trivial $t$-$(v, k, \lambda)$ design with $t \geq 2$, then we have $b \geq v$, that is, there are at least as many blocks as points in $\mathcal{D}$.*

We remark that equality holds exactly for square designs when $t = 2$. Obviously, the equality $v = b$ implies $r = k$ by Lemma 1.2 (a).

### 1.3.2. *Basic connections between codes and combinatorial designs*

There is a rich and fruitful interplay between coding theory and design theory. In particular, many $t$-designs have been found in the last decades by considering the codewords of fixed weight in some special, often linear codes. As we will see in the sequel, these codes typically exhibit a high degree of regularity. There is an amount of literature [4, 7, 13, 31, 65–72] discussing to some extent in more detail various relations between codes and designs.

For a codeword $x \in \mathbb{F}^n$, the set

$$\mathrm{supp}(x) := \{i \mid x_i \neq 0\}$$

of all coordinate positions with non-zero coordinates is called the *support* of $x$. We shall often form a $t$-design of a code in the following way: Given a (usually linear) code of length $n$, which contains the zero vector, and non-zero weight $w$, we choose as point set $X$ the set of $n$ coordinate positions of the code and as block set $\mathcal{B}$ the supports of all codewords of weight $w$.

Since we do not allow repeated blocks, clearly only distinct representatives of supports for codewords with the same supports are taken in the non-binary case.

We give some elementary examples.

**Example 1.8.** The matrix

$$G = \begin{pmatrix} 1\,1\,0\,1\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0\,0 \\ 0\,0\,1\,1\,0\,1\,0 \\ 0\,0\,0\,1\,1\,0\,1 \end{pmatrix}$$

is a generator matrix of a binary $[7, 4, 3]$ Hamming code, which is the smallest non-trivial Hamming code (see also Example 1.12). This code is a perfect single-error-correcting code with weight distribution $A_0 = A_7 = 1$, $A_3 = A_4 = 7$. The seven codewords of weight 3 are precisely the seven rows of the incidence matrix

$$\begin{pmatrix} 1\,1\,0\,1\,0\,0\,0 \\ 0\,1\,1\,0\,1\,0\,0 \\ 0\,0\,1\,1\,0\,1\,0 \\ 0\,0\,0\,1\,1\,0\,1 \\ 1\,0\,0\,0\,1\,1\,0 \\ 0\,1\,0\,0\,0\,1\,1 \\ 1\,0\,1\,0\,0\,0\,1 \end{pmatrix}$$

of the Fano plane $PG(2, 2)$ of Fig. 1.1. The supports of the seven codewords of weight 4 yield the complementary $2$-$(7, 4, 2)$ design, i.e. the biplane of order 2.

**Example 1.9.** The matrix $(I_4, J_4 - I_4)$, where $J_4$ denotes the $(4 \times 4)$ all-one matrix, generates the extended binary $[8, 4, 4]$ Hamming code. This code is self-dual and has weight distribution $A_0 = A_8 = 1$, $A_4 = 14$. As any two codewords of weight 4 have distance at least 4, they have at most two 1's in common, and hence no codeword of weight 3 can appear as a subword of more than one codeword. On the other hand, there are $\binom{8}{3} = 56$ words of weight 3 and each codeword of weight 4 has four subwords of weight 3. Hence each codeword of weight 3 is a subword of exactly one codeword of weight 4. Therefore, the supports of the fourteen codewords of weight 4 form a $3$-$(8, 4, 1)$ design, which is the unique $SQS(8)$ (cf. Example 1.5).

We give also a basic example of a non-linear code constructed from design theory.

**Example 1.10.** We take the rows of an incidence matrix of the (unique) Hadamard $2$-$(11, 5, 2)$ design, and adjoin the all-one codeword. Then, the twelve codewords have mutual distance 6, and if we delete a coordinate, we get a binary non-linear code of length 10 and minimum distance 5.

For a detailed description of the connection between non-linear codes and design theory as well as the application of design theory in the area of (majority-logic) decoding, the reader is referred, e.g., to [13, 71, 72].

Using highly transitive permutation groups, a further construction of designs from codes can be described (see, e.g., [31]).

**Theorem 1.4.** *Let $C$ be a code which admits an automorphism group acting $t$-homogeneously (in particular, $t$-transitively) on the set of coordinates. Then the supports of the codewords of any non-zero weight form a $t$-design.*

**Example 1.11.** The $r$-th order *Reed-Muller (RM) code* $\mathrm{RM}(r, m)$ of length $2^m$ is a binary $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]$ code with its codewords the value-vectors of all Boolean functions in $m$ variables of degree at most $r$. These codes were first considered by D. E. Muller [73] and I. S. Reed [74] in 1954. The dual of the Reed-Muller code $\mathrm{RM}(r, m)$ is $\mathrm{RM}(m-r-1, m)$. Clearly, the extended binary $[8, 4, 4]$ Hamming code in Example 1.9 is $\mathrm{RM}(1, 3)$.

Alternatively, a codeword in $\mathrm{RM}(r, m)$ can be viewed as the sum of characteristic functions of subspaces of dimension at least $m-r$ of the affine space $AG(m, 2)$. Thus, the full automorphism group of $\mathrm{RM}(r, m)$ contains the 3-transitive group $AGL(m, 2)$ of all affine transformations, and hence the codewords of any fixed non-zero weight yield a 3-design.

### 1.3.3. *Perfect codes and designs*

The interplay between coding theory and combinatorial designs is most evidently seen in the relationship between perfect codes and $t$-designs.

**Theorem 1.5.** (Assmus and Mattson [75]). *A linear $e$-error-correcting code of length $n$ over $\mathbb{F}_q$ is perfect if and only if the supports of the codewords of minimum weight $d = 2e + 1$ form an $(e + 1)$-$(n, d, (q - 1)^e)$ design.*

The question

> "Does every Steiner triple system on $n$ points extend to a Steiner quadruple system on $n + 1$ points?"

which goes also back to Jakob Steiner [40], is still unresolved in general. However, in terms of binary $e$-error-correcting codes, there is a positive answer.

**Theorem 1.6.** (Assmus and Mattson [75]). *Let $C$ be a (not necessarily linear) binary $e$-error correcting code of length $n$, which contains the zero vector. Then $C$ is perfect if and only if the supports of the codewords of minimum weight $d = 2e+1$ form a Steiner $(e + 1)$-$(n, d, 1)$ design. Moreover, the supports of the minimum codewords in the extended code $\overline{C}$ form a Steiner $(e + 2)$-$(n + 1, d + 1, 1)$ design.*

We have seen in Example 1.8 and Example 1.9 that the supports of the seven codewords of weight 3 in the binary $[7, 4, 3]$ Hamming code form a $STS(7)$, while the supports of the fourteen codewords of weight 4 in the extended $[8, 4, 4]$ Hamming

code yield a $SQS(8)$. In view of the above theorems, we get more generally:

**Example 1.12.** Let $n := (q^m - 1)/(q - 1)$. We consider a $(m \times n)$-matrix $H$ over $\mathbb{F}_q$ such that no two columns of $H$ are linearly dependent. Then $H$ clearly is a parity check matrix of an $[n, n - m, 3]$ code, which is the *Hamming code* over $\mathbb{F}_q$. The number of its codewords is $q^{n-m}$, and for any codeword $\mathbf{x}$, we have $S_1(\mathbf{x}) = 1 + n(q-1) = q^m$. Hence, by the Sphere Packing Bound (Theorem 1.1), this code is perfect, and the supports of codewords of minimum weight 3 form a 2-$(n, 3, q - 1)$ design. Furthermore, in a binary $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code the supports of codewords of weight 3 form a $STS(2^m - 1)$, and the supports of the codewords of weight 4 in the extended code yield a $SQS(2^m)$.

**Note.** The Hamming codes were developed by R. W. Hamming [2] in the mid 1940's, who was employed at Bell Laboratories, and addressed a need for error correction in his work on the primitive computers of the time. We remark that the extended binary $[2^m, 2^m - m - 1, 4]$ Hamming code is the Reed-Muller code $\mathrm{RM}(m - 2, m)$.

**Example 1.13.** The *binary Golay code* is a $[23, 12, 7]$ code, while the *ternary Golay code* is a $[11, 6, 5]$ code. For both codes, the parameters imply equality in the Sphere Packing Bound, and hence these codes are perfect. We will discuss later various constructions of these some of the most famous codes (see Example 1.14 and Construction 1.12). By the above theorems, the supports of codewords of minimum weight 7 in the binary $[23, 12, 7]$ Golay code form a Steiner 4-$(23, 7, 1)$ design, and the supports of the codewords of weight 8 in the extended binary $[24, 12, 8]$ Golay code give a Steiner 5-$(24, 8, 1)$ design. The supports of codewords of minimum weight 5 in the ternary $[11, 6, 5]$ Golay code yield a 3-$(11, 5, 4)$ design. It can be shown (e.g., via Theorem 1.4) that this is indeed a Steiner 4-$(11, 5, 1)$ design. We will see in Example 1.15 that the supports of the codewords of weight 6 in the extended ternary $[12, 6, 6]$ Golay code give a Steiner 5-$(12, 6, 1)$ design; thus the above results are not best possible.

**Note.** The Golay codes were discovered by M. J. E. Golay [76] in 1949 in the process of extending Hamming's construction. They have numerous practical real-world applications, e.g., the use of the extended binary Golay code in the Voyager spacecraft program during the early 1980's or in contemporary standard Automatic Link Establishment (ALE) in High Frequency (HF) data communication for Forward Error Correction (FEC).

**Remark 1.4.** It is easily seen from their construction that the Hamming codes are unique (up to equivalence). It was shown by V. Pless [77] that this is also true for the Golay codes. Moreover, the binary and ternary Golay codes are the only non-trivial perfect $e$-error-correcting codes with $e > 1$ over any field $\mathbb{F}_q$. Using integral roots of the Lloyd polynomial, this remarkable fact was proven by A. Tietäväinen [78] and

J. H. van Lint [79], and independently by V. A. Zinov'ev and V. K. Leont'ev [80].
M. R. Best [81] and Y. Hong [82] extended this result to arbitrary alphabets for
$e > 2$. For a thorough account of perfect codes, we refer to [83] and [84, Chap. 11].

As trivial perfect codes can only form trivial designs, we have (up to equivalence)
a complete list of non-trivial linear perfect codes with their associated designs:

| Code | Code parameters | | Design parameters |
|---|---|---|---|
| Hamming code | $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3]$ | $q$ any prime power | $2\text{-}(\frac{q^m-1}{q-1}, 3, q-1)$ |
| binary Golay code | $[23, 12, 7]$ | $q = 2$ | $4\text{-}(23, 7, 1)$ |
| ternary Golay code | $[11, 6, 5]$ | $q = 3$ | $4\text{-}(11, 5, 1)$ |

There are various constructions of non-linear single-error-correcting perfect
codes. For more details, see, e.g., [9, 13, 71, 72, 85] and references therein. However,
a classification of these codes seems out of reach at present, although some progress
has been made recently, see, for instance [86–88].

**Remark 1.5.** The long-standing question whether every Steiner triple system of
order $2^m - 1$ occurs in a perfect code has been answered recently in the negative.
Relying on the classification [89] of the Steiner quadruple systems of order 16, it was
shown in [90] that the unique anti-Pasch Steiner triple system of order 15 provides
a counterexample.

**Remark 1.6.** Due to the close relationship between perfect codes and some of
the most interesting designs, several natural extensions of perfect codes have been
examined in this respect: *Nearly perfect codes* [91], and the more general class
of *uniformly packed codes* [92, 93], were studied extensively and eventually lead
to $t$-designs. H. C. A. van Tilborg [94] showed that $e$-error correcting uniformly
packed codes do not exist for $e > 3$, and classified those for $e \leq 3$. For more
details, see [4, 10, 13, 94]. The concept of *diameter perfect codes* [95, 96] is related
particularly to Steiner designs. For further generalizations of perfect codes, see
e.g., [84, Chap. 11] and [13, Chap. 6].

### 1.3.4. *The Assmus-Mattson Theorem and analogues*

We consider in this subsection one of the most fundamental results in the interplay
of coding theory and design theory. We start by introducing two important classes
of codes.

Let $q$ be an odd prime power. We define a function $\chi$ (the so-called *Legendre-
symbol*) on $\mathbb{F}_q$ by

$$\chi(x) := \begin{cases} 0, & \text{if } x = 0 \\ 1, & \text{if } x \text{ is a non-zero square} \\ -1, & \text{otherwise.} \end{cases}$$

We note that $\chi$ is a character on the multiplicative group of $\mathbb{F}_q$. Using the elements of $\mathbb{F}_q$ as row and column labels $a_i$ and $a_j$ $(0 \leq i, j < q)$, respectively, a matrix $Q = (q_{ij})$ of order $q$ can be defined by

$$q_{ij} := \chi(a_j - a_i). \tag{1.1}$$

If $q$ is a prime, then $Q$ is a circulant matrix. We call a matrix

$$C_{q+1} := \begin{pmatrix} 0 & 1 & \cdots & 1 \\ \chi(-1) & & & \\ \vdots & & Q & \\ \chi(-1) & & & \end{pmatrix}$$

of order $q + 1$ a *Paley matrix*. These matrices were constructed by R. A. Paley in 1933 and are a specific type of conference matrices, which have their origin in the application to conference telephone circuits.

**Construction 1.7.** Let $n$ be an odd prime, and $q$ be a *quadratic residue* (mod $n$), i.e. $q^{(n-1)/2} \equiv 1$ (mod $n$). The *quadratic residue code* (or *QR code*) of length $n$ over $\mathbb{F}_q$ is a $[n, (n+1)/2]$ code with minimum weight $d \geq \sqrt{n}$ (so-called *Square Root Bound*). It can be generated by the $(0,1)$-circulant matrix of order $n$ with top row the incidence vector of the non-zero quadratic residues (mod $n$). These codes are a special class of cyclic codes and were first constructed by A. M. Gleason in 1964. For $n \equiv 3$ (mod 4), the extended quadratic residue code is self-dual. We note for the important binary case that $q$ is a quadratic residue (mod $n$) if and only if $n \equiv \pm 1$ (mod 8).

**Note.** By a theorem of A. M. Gleason and E. Prange, the full automorphism group of an extended quadratic residue code of length $n$ contains the group $PSL(2, n)$ of all linear fractional transformations whose determinant is a non-zero square.

**Example 1.14.** The binary $[7, 4, 3]$ Hamming code is a quadratic residue code of length 7 over $\mathbb{F}_2$. The binary $[23, 12, 7]$ Golay code is a quadratic residue code of length 23 over $\mathbb{F}_2$, while the ternary $[11, 6, 5]$ Golay code is a quadratic residue code of length 11 over $\mathbb{F}_3$.

**Construction 1.8.** For $q \equiv -1$ (mod 6) a prime power, the *Pless symmetry code* $\mathrm{Sym}_{2(q+1)}$ of dimension $q+1$ is a ternary $[2(q+1), q+1]$ code with generator matrix $G_{2(q+1)} := (I_{q+1}, C_{q+1})$, where $C_{q+1}$ is a Paley matrix. Since $C_{q+1}C_{q+1}^T = -I_{q+1}$ (over $\mathbb{F}_3$) for $q \equiv -1$ (mod 3), the code $\mathrm{Sym}_{2(q+1)}$ is self-dual. This infinite family of cyclic codes were introduced by V. Pless [97, 98] in 1972. We note that the first symmetry code $S_{12}$ is equivalent to the extended $[12, 6, 6]$ Golay code.

The celebrated Assmus-Mattson Theorem gives a sufficient condition for the codewords of constant weight in a linear code to form a $t$-design.

**Theorem 1.9.** (Assmus and Mattson [99]). *Let $C$ be an $[n, k, d]$ code over $\mathbb{F}_q$ and $C^\perp$ be the $[n, n-k, e]$ dual code. Let $n_0$ be the largest integer such that $n_0 - \frac{n_0+q-2}{q-1} < d$, and define $m_0$ similarly for the dual code $C^\perp$, whereas if $q = 2$, we assume that $n_0 = m_0 = n$. For some integer $t$ with $0 < t < d$, let us suppose that there are at most $d - t$ non-zero weights $w$ in $C^\perp$ with $w \leq n - t$. Then, for any weight $v$ with $d \leq v \leq n_0$, the supports of codewords of weight $v$ in $C$ form a $t$-design. Furthermore, for any weight $w$ with $e \leq w \leq \min\{n - t, m_0\}$, the support of the codewords $w$ in $C^\perp$ also form a $t$-design.*

The proof of the theorem involves a clever use of the MacWilliams relations (Theorem 1.2). Along with these, Lemma 1.1 and the immediate observation that codewords of weight less than $n_0$ with the same support must be scalar multiples of each other, form the basis of the proof (for a detailed proof, see, e.g., [4, Chap. 14]).

**Remark 1.7.** Until this result by E. F. Assmus, Jr. and H. F. Mattson, Jr. in 1969, only very few 5-designs were known: the Mathieu-Witt designs 5-$(12, 6, 1)$ and 5-$(24, 8, 1)$, the 5-$(24, 8, 48)$ design formed by the codewords of weight 12 (the *dodecads*) in the extended binary Golay code, as well as 5-$(12, 6, 2)$ and 5-$(24, 8, 2)$ designs which had been found without using coding theory. However, by using the Assmus-Mattson Theorem, it was possible to find a number of new 5-designs. In particular, the theorem is most useful when the dual code has relatively few non-zero weights. Nevertheless, it has not been possible to detect $t$-designs for $t > 5$ by the Assmus-Mattson Theorem.

We illustrate in the following examples some applications of the theorem.

**Example 1.15.** The extended binary $[24, 12, 8]$ Golay code is self-dual (cf. Construction 1.7) and has codewords of weight $0, 8, 12, 16$, and 24 in view of Theorem 1.2. For $t = 5$, we obtain the Steiner 5-$(24, 8, 1)$ design as in Example 1.13. In the self-dual extended ternary $[12, 6, 6]$ Golay code all codewords are divisible by 3, and hence for $t = 5$, the supports of the codewords of weight 6 form a Steiner 5-$(12, 6, 1)$ design.

**Example 1.16.** The extended quadratic residue code of length 48 over $\mathbb{F}_2$ is self-dual with minimum distance 12. By Theorem 1.2, it has codewords of weight $0, 12, 16, 20, 24, 28, 32, 36$, and 48. For $t = 5$, each of the values $v = 12, 16, 20$, or 24 yields a different 5-design and its complementary design.

**Example 1.17.** The Pless symmetry code $\text{Sym}_{36}$ of dimension 18 is self-dual (cf. Construction 1.8) with minimum distance 12. The supports of codewords of weight $12, 15, 18$, and 21 yield 5-designs together with their complementary designs.

**Remark 1.8.** We give an overview of the state of knowledge concerning codes over $\mathbb{F}_q$ with their associated 5-designs (cf. also the tables in [13, Chap. 16], [65, 71, 72]). In fact, these codes are all self-dual. Trivial designs as well as complementary designs are omitted.

| Code | Code parameters | | Design parameters | Ref. |
|---|---|---|---|---|
| Extended cyclic code | $[18, 9, 8]$ | $q = 4$ | 5-$(18, 8, 6)$ | [100] |
| | | | 5-$(18, 10, 180)$ | |
| Extended binary Golay code | $[24, 12, 8]$ | $q = 2$ | 5-$(24, 8, 1)$ | [101] |
| | | | 5-$(24, 12, 48)$ | |
| Extended ternary Golay code | $[12, 6, 6]$ | $q = 3$ | 5-$(12, 6, 1)$ | |
| Lifted Golay code over $\mathbb{Z}_4$ | $[24, 12]$ | $\mathbb{Z}_4$ | 5-$(24, 10, 36)$ | [102, 103] |
| | | | 5-$(24, 11, 336)$ | [102] |
| | | | 5-$(24, 12, 1584)$ | [102] |
| | | | 5-$(24, 12, 1632)$ | [102] |
| Extended quadric residue codes | $[24, 12, 9]$ | $q = 3$ | 5-$(24, 9, 6)$ | [65, 99] |
| | | | 5-$(24, 12, 576)$ | |
| | | | 5-$(24, 15, 8580)$ | |
| | $[30, 15, 12]$ | $q = 4$ | 5-$(30, 12, 220)$ | [65, 99] |
| | | | 5-$(30, 14, 5390)$ | |
| | | | 5-$(30, 16, 123000)$ | |
| | $[48, 24, 12]$ | $q = 2$ | 5-$(48, 12, 8)$ | [65, 99] |
| | | | 5-$(48, 16, 1365)$ | |
| | | | 5-$(48, 20, 36176)$ | |
| | | | 5-$(48, 24, 190680)$ | |
| | $[48, 24, 15]$ | $q = 3$ | 5-$(48, 12, 364)$ | [65, 99] |
| | | | 5-$(48, 18, 50456)$ | |
| | | | 5-$(48, 21, 2957388)$ | |
| | | | 5-$(48, 24, 71307600)$ | |
| | | | 5-$(48, 27, 749999640)$ | |
| | $[60, 30, 18]$ | $q = 3$ | 5-$(60, 18, 3060)$ | [65, 99] |
| | | | 5-$(60, 21, 449820)$ | |
| | | | 5-$(60, 24, 34337160)$ | |
| | | | 5-$(60, 27, 1271766600)$ | |
| | | | 5-$(60, 30, 24140500956)$ | |
| | | | 5-$(60, 33, 239329029060)$ | |
| Pless symmetry codes | $[24, 12, 9]$ | $q = 3$ | 5-$(24, 9, 6)$ | [98] |
| | | | 5-$(24, 12, 576)$ | |
| | | | 5-$(24, 15, 8580)$ | |
| | $[36, 18, 12]$ | $q = 3$ | 5-$(36, 12, 45)$ | [98] |
| | | | 5-$(36, 15, 5577)$ | |
| | | | 5-$(36, 18, 209685)$ | |
| | | | 5-$(36, 21, 2438973)$ | |
| | $[48, 24, 15]$ | $q = 3$ | 5-$(48, 12, 364)$ | [98] |
| | | | 5-$(48, 18, 50456)$ | |
| | | | 5-$(48, 21, 2957388)$ | |
| | | | 5-$(48, 24, 71307600)$ | |
| | | | 5-$(48, 27, 749999640)$ | |
| | $[60, 30, 18]$ | $q = 3$ | 5-$(60, 18, 3060)$ | [97, 98] |
| | | | 5-$(60, 21, 449820)$ | |
| | | | 5-$(60, 24, 34337160)$ | |
| | | | 5-$(60, 27, 1271766600)$ | |
| | | | 5-$(60, 30, 24140500956)$ | |
| | | | 5-$(60, 33, 239329029060)$ | |

**Note.** The lifted Golay code over $\mathbb{Z}_4$ is defined in [104] as the extended Hensel lifted quadric residue code of length 24. The supports of the codewords of Hamming weight 10 in the lifted Golay code and certain extremal double circulant Type II

codes of length 24 yield (non-isomorphic) 5-$(24, 10, 36)$ designs. We further note that the quadratic residue codes and the Pless symmetry codes listed in the table with the same parameters are not equivalent as shown in [98] by inspecting specific elements of the automorphism group $PSL(2, q)$.

**Remark 1.9.** The concept of the weight enumerator can be generalized to non-linear codes (so-called *distance enumerator*), which leads to an analog of the MacWilliams relations as well as to similar results to the Assmus-Mattson Theorem for non-linear codes (see [17, 18, 105] and Subsection 1.3.8). The question whether there is an analogous result to the Assmus-Mattson theorem for codes over $\mathbb{Z}_4$ proposed in [102] was answered in the affirmative in [106]. Further generalizations of the Assmus-Mattson Theorem are known, see in particular [107–113].

### 1.3.5. *Codes and finite geometries*

Let $A$ be an incidence matrix of a projective plane $PG(2, n)$ of order $n$. When we consider the subspace $C$ of $\mathbb{F}_2^{n^2+n+1}$ spanned by the rows of $A$, we obtain for odd $n$ only the $[n^2 + n + 1, n^2 + n, 2]$ code consisting of all codewords of even weight. The case for even $n$ is more interesting, in particular if $n \equiv 2 \pmod 4$.

**Theorem 1.10.** *For $n \equiv 2 \pmod 4$, the rows of an incidence matrix of a projective plane $PG(2, n)$ of order $n$ generate a binary code $C$ of dimension $(n^2 + n + 2)/2$, and the extended code $\overline{C}$ is self-dual.*

In a projective plane $PG(2, n)$ of even order $n$, there exist sets of $n + 2$ points, no three of which are collinear, and which are called *hyperovals* (sometimes just *ovals*, cf. [46]). This gives furthermore

**Theorem 1.11.** *The code $C$ has minimum weight $n+1$. Moreover, the codewords of minimum weight correspond to the lines and those of weight $n + 2$ to the hyperovals of $PG(2, n)$.*

**Remark 1.10.** The above two theorems arose in the context of the examination of the existence of a projective plane of order 10 (cf. Remark 1.1; for detailed proofs see, e.g., [4, Chapt. 13]). Assuming the existence of such a plane, the obtained properties of the corresponding code lead to very extensive computer searches. For example, in an early crucial step, it was shown [114] that this code could not have codewords of weight 15. On the various attempts to attack the problem and the final verification of the non-existence, we refer to [44, 115, 116] as well as [22, Chap. 17] and [35, Chap. 12].

**Note.** We note that at present the Fano plane is the only known projective plane with order $n \equiv 2 \pmod 4$.

For further accounts on codes and finite geometries, the reader is referred, e.g., to [66, Chap. 5 and 6] and [3, 4, 67, 116–119], as well as [120] from a more group-theoretical perspective and [121] with an emphasis on quadratic forms over $\mathbb{F}_2$.

### 1.3.6.  *Golay codes, Mathieu-Witt designs, and Mathieu groups*

We highlight some of the remarkable and natural interrelations between the Golay codes, the Mathieu-Witt designs, and the Mathieu groups.

There are various different constructions for the Golay codes besides the description as quadratic residue codes in Example 1.14. We briefly illustrate some exemplary constructions. For further details and more constructions, we refer to [122], [13, Chap. 20], [4, Chap. 11], and [123, Chap. 11].

**Construction 1.12.**

- Starting with the zero vector in $\mathbb{F}_2^{24}$, a linear code of length 24 can be obtained by successively taking the lexicographically least binary codeword which has not been used and which has distance at least 8 to any predecessor. At the end of this process, we have 4096 codewords which form the extended binary Golay code. This construction is due to J. H. Conway and N. J. A. Sloane [124].
- Let $A$ be an incidence matrix of the (unique) 2-(11, 6, 3) design. Then $G := (I_{12}, P)$ with

$$P := \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{pmatrix}$$

  is a $(12 \times 24)$-matrix in which each row (except the top row) has eight 1's, and generates the extended binary Golay code.
- Let $N$ be an $(12 \times 12)$-adjacency matrix of the graph formed by the vertices and edges of the regular icosahedron. Then $G := (I_{12}, J_{12} - N)$ is a generator matrix for the extended binary Golay code.
- We recall that $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ is the field of four elements with $\omega^2 = \omega + 1$. The *hexacode* is the $[6, 3, 4]$ code over $\mathbb{F}_4$ generated by the matrix $G := (I_3, P)$ with

$$P := \begin{pmatrix} 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \\ 1 & 1 & 1 \end{pmatrix}.$$

  The extended binary Golay code can be defined by identifying each codeword with a binary $(4 \times 6)$-matrix $M$ (with rows $\mathbf{m}_0, \mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3$), satisfying

  (i)  each column of $M$ has the same parity as the first row $\mathbf{m}_0$,
  (ii) the sum $\mathbf{m}_1 + \omega \mathbf{m}_2 + \omega^2 \mathbf{m}_3$ lies in the hexacode.

This description is essentially equivalent to the computational tool *MOG (Miracle Octad Generator)* of R. T. Curtis [125]. The construction via the hexacode is by Conway, see, e.g., [123, Chap. 11].

- Let $Q$ be the circulant matrix of order 5 defined by Eq. (1.1). Then $G := (I_6, P)$, where $P$ is the matrix $Q$ bordered on top with a row of 1's, is a generator matrix of the ternary Golay code.

**Remark 1.11.** Referring to Example 1.7, we note that the automorphism groups of the Golay codes are isomorphic to the particular Mathieu groups, as was first pointed out in [101, 126]. Moreover, the Golay codes are related in a particularly deep and interesting way to a larger family of sporadic finite simple groups (cf., e.g., [55]).

**Remark 1.12.** We have seen in Example 1.13 that the supports of the codewords of weight 8 in the extended binary $[24, 12, 8]$ Golay code form a Steiner 5-$(24, 8, 1)$ design. The uniqueness of the large Mathieu-Witt design (up to isomorphism) can be established easily via coding theory (cf. Example 1.7). The main part is to show that any binary code of 4096 codewords, including the zero vector, of length 24 and minimum distance 8, is linear and can be determined uniquely (up to equivalence). For further details, in particular for a uniqueness proof of the small Mathieu-Witt designs, see, e.g., [70, 122] and [4, Chap. 11].

### 1.3.7. *Golay codes, Leech lattice, kissing numbers, and sphere packings*

Sphere packings closely connect mathematics and information theory via the sampling theorem as observed by C. E. Shannon [1] in his classical article of 1948. Rephrased in a more geometric language, this can be expressed as follows:

> "Nearly equal signals are represented by neighboring points, so to keep the signals distinct, Shannon represents them by $n$-dimensional 'billiard balls', and is therefore led to ask: what is the best way to pack 'billiard balls' in $n$ dimensions?" [127]

One of the most remarkable lattices, the *Leech lattice* in $\mathbb{R}^{24}$, plays a crucial role in classical sphere packings. We recall that a *lattice* in $\mathbb{R}^n$ is a discrete subgroup of $\mathbb{R}^n$ of rank $n$. The extended binary Golay code led to the discovery by John Leech [128] of the 24-dimensional Euclidean lattice named after him. There are various constructions besides the usual ones from the binary and ternary Golay codes in the meantime, see, e.g., [129], [123, Chap. 24]. We outline some of the fundamental connections between sphere packings and the Leech lattice.

The *Kissing Number Problem* deals with the maximal number $\tau_n$ of equal size non-overlapping spheres in the $n$-dimensional Euclidean space $\mathbb{R}^n$ that can touch a given sphere of the same size. Only a few of these numbers are actually known. For dimensions $n = 1, 2, 3$, the classical solutions are: $\tau_1 = 2$, $\tau_2 = 6$, $\tau_3 = 12$. The number $\tau_3$ was the subject of a famous controversy between Isaac Newton and

David Gregory in 1694, and was finally verified only in 1953 by K. Schütte and B. L. van der Waerden [130]. Using an approach initiated by P. Delsarte [18, 131] in the early 1970's which gives linear programming upper bounds for binary error-correcting codes and for spherical codes [132] (cf. Subsection 1.3.8), A. M. Odlyzko and N. J. A. Sloane [133], and independently V. I. Levenshtein [134], proved that $\tau_8 = 240$ and $\tau_{24} = 196560$. These exact solutions are the number of non-zero vectors of minimal length in the root lattice $E_8$ and in the Leech lattice, respectively. By extending and improving Delsarte's method, O. R. Musin [135] verified in 2003 that $\tau_4 = 24$, which is the number of non-zero vectors of minimal length in the root lattice $D_4$.

The *Sphere Packing Problem* asks for the maximal density of a packing of equal size non-overlapping spheres in the $n$-dimensional Euclidean space $\mathbb{R}^n$. A sphere packing is called a *lattice packing* if the centers of the spheres form a lattice in $\mathbb{R}^n$. The Leech lattice is the unique densest lattice packing (up to scaling and isometries) in $\mathbb{R}^{24}$, as was shown by H. Cohn and A. Kumar [136, 137] recently in 2004, again by a modification of Delsarte's method. Moreover, they showed that the density of any sphere packing in $\mathbb{R}^{24}$ cannot exceed the one given by the Leech lattice by a factor of more than $1 + 1.65 \cdot 10^{-30}$ (via a computer calculation). The proof is based on the work [138] by Cohn and N. D. Elkies in 2003 in which linear programming bounds for the Sphere Packing Problem are introduced and new upper bounds on the density of sphere packings in $\mathbb{R}^n$ with dimension $n \leq 36$ are proven.

For further details on the Kissing Number Problem and the Sphere Packing Problem, see [123, Chap. 1], [127, 139], [14], as well as the survey articles [140–142]. For an on-line database on lattices, see [143].

### 1.3.8. *Codes and association schemes*

Any finite nonempty subset of the unit sphere $S^{n-1}$ in the $n$-dimensional Euclidean space $\mathbb{R}^n$ is called a *spherical code*. These codes have many practical applications, e.g., in the design of signals for data transmission and storage. As a special class of spherical codes, *spherical designs* were introduced by P. Delsarte, J.-M. Goethals and J. Seidel [132] in 1977 as analogs on $S^{n-1}$ of the classical combinatorial designs. For example, in $S^2$ the tetrahedron is a spherical 2-design; the octahedron and the cube are spherical 3-designs, and the icosahedron and the dodecahedron are spherical 5-designs. In order to obtain the linear programming upper bound mentioned in the previous subsection, Krawtchouk polynomials were involved in the case of binary error-correcting codes and Gegenbauer polynomials in the case of spherical codes.

However, Delsarte's approach was indeed much more general and far-reaching. He developed for association schemes, which have their origin in the statistical theory of design of experiments, a theory to unify many of the objects we have been addressing in this chapter. We give a formal definition of *association schemes*

in the sense of Delsarte [18] as well as introduce the *Hamming* and the *Johnson schemes* as important examples of the two fundamental classes of *P-polynomial* and *Q-polynomial association schemes*.

**Definition 1.3.** A *d-class association scheme* is a finite point set $X$ together with $d+1$ relations $R_i$ on $X$, satisfying

(i) $\{R_0, R_1, \ldots, R_d\}$ is a partition of $X \times X$,

(ii) $R_0 = \{(x,x) \mid x \in X\}$,

(iii) for each $i$ with $0 \leq i \leq d$, there exists a $j$ with $0 \leq j \leq d$ such that $(x,y) \in R_i$ implies $(y,x) \in R_j$,

(iv) for any $(x,y) \in R_k$, the number $p_{ij}^k$ of points $z \in X$ with $(x,z) \in R_i$ and $(z,y) \in R_j$ depends only on $i, j$ and $k$,

(v) $p_{ij}^k = p_{ji}^k$ for all $i$, $j$ and $k$.

The numbers $p_{ij}^k$ are called the *intersection numbers* of the association scheme. Two points $x, y \in X$ are called *i-th associates* if $\{x, y\} \in R_i$.

**Example 1.18.** The *Hamming scheme* $H(n,q)$ has as point set $X$ the set $\mathbb{F}^n$ of all $n$-tuples from a $q$-symbol alphabet; two $n$-tuples are $i$-th associates if their Hamming distance is $i$. The *Johnson scheme* $J(v,k)$, with $k \leq \frac{1}{2}v$, has as point set $X$ the set of all $k$-element subsets of a set of size $v$; two $k$-element subset $S_1, S_2$ are $i$-th associates if $|S_1 \cap S_2| = k - i$.

Delsarte introduced the Hamming and Johnson schemes as settings for the classical concept of error-correcting codes and combinatorial $t$-designs, respectively. In this manner, certain results become formally dual, like the Sphere Packing Bound (Theorem 1.1) and Fisher's Inequality (Theorem 1.3).

For a more extended treatment of association schemes, the reader is referred, e.g., to [144–148], [4, Chap. 17], [13, Chap. 21], and in particular to [149, 150] with an emphasis on the close connection between coding theory and associations schemes. For a survey on spherical designs, see [21, Chap. VI.54].

## 1.4. Directions for further research

We present in this section a collection of significant open problems and challenges concerning future research.

**Problem 1.1.** (cf. [40]). Does every Steiner triple system on $n$ points extend to a Steiner quadruple system on $n+1$ points?

**Problem 1.2.** Does there exist any non-trivial Steiner 6-design?

**Problem 1.3.** (cf. [13, p. 180]). Find all non-linear single-error-correcting perfect codes over $\mathbb{F}_q$.

**Problem 1.4.** (cf. [6, p. 106]). Characterize codes where all codewords of the same weight (or of minimum weight) form a non-trivial design.

**Problem 1.5.** (cf. [6, p. 116]). Find a proof of the non-existence of a projective plane of order 10 without the help of a computer or with an easily reproducible computer program.

**Problem 1.6.** Does there exist any finite projective plane of order 12, or of any other order that is neither a prime power nor covered by the Bruck-Ryser Theorem (cf. Remark 1.1)?

**Problem 1.7.** Does the root lattice $D_4$ give the unique kissing number configuration in $\mathbb{R}^4$?

**Problem 1.8.** Solve the Kissing Number Problem in $n$ dimensions for any $n > 4$ apart from $n = 8$ and 24. For presently known lower and upper bounds, we refer to [151] and [152], respectively. Also any improvements of these bounds would be desirable.

**Problem 1.9.** (cf. [138, Conj. 8.1]). Verify the conjecture that the Leech lattice is the unique densest sphere packing in $\mathbb{R}^{24}$.

### 1.5. Conclusions

Over the last sixty years a substantial amount of research has been inspired by the various interactions of coding theory and algebraic combinatorics. The fruitful interplay often reveals the high degree of regularity of both the codes and the combinatorial structures. This has lead to a vivid area of research connecting closely mathematics with information and coding theory. The emerging methods can be applied sometimes surprisingly effectively, e.g., in view of the recent advances on kissing numbers and sphere packings.

A further development of this beautiful interplay as well as its application to concrete problems would be desirable, certainly also in view of the various still open and long-standing problems.

### 1.6. Terminologies/Keywords

Error-correcting codes, combinatorial designs, perfect codes and related concepts, Assmus-Mattson Theorem and analogues, projective geometries, non-existence of a projective plane of order 10, Golay codes, Leech lattice, kissing numbers, sphere packings, spherical codes, association schemes.

### 1.7. Exercises

(1) Verify (numerically) that the Steiner quadruple system $SQS(8)$ of order 8 (cf. Example 1.5) has 14 blocks, and that the Mathieu-Witt design 5-$(24, 8, 1)$ (cf. Example 1.7) has 759 blocks.

(2) What are the parameters of the 2-design consisting of the points and hyperplanes (i.e. the $(d-2)$-dimensional projective subspaces) of the projective space $PG(d - 1, q)$?

(3) Does there exist a self-dual $[8, 4]$ code over the finite field $\mathbb{F}_2$?

(4) Show that the ternary $[11, 6, 5]$ Golay code has 132 codewords of weight 5.

(5) Compute the weight distribution of the binary $[23, 12, 7]$ Golay code.

(6) Show that any binary code of 4096 codewords, including the zero vector, of length 24 and minimum distance 8 is linear.

(7) Give a proof for the Sphere Packing Bound (cf. Theorem 1.1).

(8) Give a proof for Fisher's Inequality (cf. Theorem 1.3).

(9) Show that a binary code generated by the rows of an incidence matrix of any projective plane $PG(2, n)$ of even order $n$ has dimension at most $(n^2 + n + 2)/2$ (cf. Theorem 1.10).

(10) (Todd's Lemma). In the Mathieu-Witt design 5-$(24, 8, 1)$, if $B_1$ and $B_2$ are blocks (*octads*) meeting in four points, then $B_1 + B_2$ is also a block.

### Solutions:

ad (1): By Lemma 1.2 (b), we have to calculate $b = \frac{8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2} = 14$ in the case of the Steiner quadruple system $SQS(8)$, and $b = \frac{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20}{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4} = 759$ in the case of the Mathieu-Witt design 5-$(24, 8, 1)$.

ad (2): Starting from Example 1.3, we obtain via counting arguments (or by using the transitivity properties of the general linear group) that the points and hyperplanes of the projective space $PG(d - 1, q)$ form a 2-$(\frac{q^d - 1}{q - 1}, \frac{q^{d-1} - 1}{q - 1}, \frac{q^{d-2} - 1}{q - 1})$ design.

ad (3): Yes, the extended binary $[8, 4, 4]$ Hamming code is self-dual (cf. Example 1.9).

ad (4): Since the ternary $[11, 6, 5]$ Golay code is perfect (cf. Example 1.13), every word of weight 3 in $\mathbb{F}_3^{11}$ has distance 2 to a codeword of weight 5. Thus $A_5 = 2^3 \cdot \binom{11}{3} / \binom{5}{2} = 132$.

ad (5): The binary $[23, 12, 7]$ Golay code contains the zero vector and is perfect. This determines the weight distribution as follows $A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$, $A_{11} = A_{12} = 1288$.

ad (6): Let $C$ denote a binary code of 4096 codewords, including the zero vector, of length 24 and minimum distance 8. Deleting any coordinate leads to a code

which has the same weight distribution as the code given in Exercise (5). Hence, the code $C$ only has codewords of weight $0, 8, 12, 16$ and $24$. This is still true if the code $C$ is translated by any codeword (i.e. $C + \mathbf{x}$ for any $\mathbf{x} \in C$). Thus, the distances between pairs of codewords are also $0, 8, 12, 16$ and $24$. Therefore, the standard inner product $\langle \mathbf{x}, \mathbf{y} \rangle$ vanishes for any two codewords $\mathbf{x}, \mathbf{y} \in C$, and hence $C$ is self-orthogonal. For cardinality reasons, we conclude that $C$ is self-dual and hence in particular linear.

ad (7): The sum $\sum_{i=0}^{e} \binom{n}{i}(q-1)^i$ counts the number of words in a sphere of radius $e$. As the spheres of radius $e$ about distinct codewords are disjoint, we obtain $|C| \cdot \sum_{i=0}^{e} \binom{n}{i}(q-1)^i$ words. Clearly, this number cannot exceed the total number $q^n$ of words, and the claim follows.

ad (8): As a non-trivial $t$-design with $t \geq 2$ is also a non-trivial 2-design by Lemma 1.1, it is sufficient to prove the assertion for an arbitrary non-trivial 2-$(v, k, \lambda)$ design $\mathcal{D}$. Let $A$ be an incidence matrix of $\mathcal{D}$ as defined in Subsection 1.3.1. Clearly, the $(i, k)$-th entry

$$(AA^t)_{ik} = \sum_{j=1}^{b} (A)_{ij}(A^t)_{jk} = \sum_{j=1}^{b} a_{ij}a_{kj}$$

of the $(v \times v)$-matrix $AA^t$ is the total number of blocks containing both $x_i$ and $x_k$, and is thus equal to $r$ if $i = k$, and to $\lambda$ if $i \neq k$. Hence

$$AA^t = (r - \lambda)I + \lambda J,$$

where $I$ denotes the $(v \times v)$-unit matrix and $J$ the $(v \times v)$-matrix with all entries equal to 1. Using elementary row and column operations, it follows easily that

$$\det(AA^t) = rk(r - \lambda)^{v-1}.$$

Thus $AA^t$ is non-singular (i.e. its determinant is non-zero) as $r = \lambda$ would imply $v = k$ by Lemma 1.1, yielding that the design is trivial. Therefore, the matrix $AA^t$ has rank$(A) = v$. But, if $b < v$, then rank$(A) \leq b < v$, and thus rank$(AA^t) < v$, a contradiction. It follows that $b \geq v$, proving the claim.

ad (9): Let $C$ denote a binary code generated by the rows of an incidence matrix of $PG(2, n)$. By assumption $n$ is even, and hence the extended code $\overline{C}$ must be self-orthogonal. Therefore, the dimension of $C$ is at most $n^2 + n + 2/2$.

ad (10): For given blocks $B_1 = \{01, 02, 03, 04, 05, 06, 07, 08\}$ and $B_2 = \{01, 02, 03, 04, 09, 10, 11, 12\}$ in the Mathieu-Witt design 5-$(24, 8, 1)$, let us assume that $B_1 + B_2$ is not a block. The block $B_3$ which contains $\{05, 06, 07, 08, 09\}$ must contain just one more point of $B_2$, say $B_3 = \{05, 06, 07, 08, 09, 10, 13, 14\}$. Similarly, $B_4 = \{05, 06, 07, 08, 11, 12, 15, 16\}$ is the block containing $\{05, 06, 07, 08, 11\}$. But hence, it is impossible to find a block which contains $\{05, 06, 07, 09, 11\}$ and intersects with $B_i$, $1 \leq i \leq 4$, in 0, 2 or 4 points. Therefore, we obtain a contradiction as there must be a block containing any five points by Definition 1.2.

# References

[1] C. E. Shannon, A mathematical theory of communication, *Bell Syst. Tech. J.* **27**, 379–423 and 623–656, (1948).

[2] R. W. Hamming, Error detecting and error correcting codes, *Bell Syst. Tech. J.* **29**, 147–160, (1950).

[3] E. R. Berlekamp, *Algebraic Coding Theory*. (McGraw-Hill, New York, 1968; Revised edition: Aegean Park Press 1984).

[4] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*. (Cambridge Univ. Press, Cambridge, 1991).

[5] R. Hill, *A First Course in Coding Theory*. (Clarendon Press, Oxford, 1986).

[6] W. C. Huffman and V. Pless, Eds., *Handbook of Coding Theory*. vol. I and II, (North-Holland, Amsterdam, New York, Oxford, 1998).

[7] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. (Cambridge Univ. Press, Cambridge, 2003).

[8] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-Correcting Linear Codes*. (Springer, Berlin, Heidelberg, New York, 2006).

[9] J. H. van Lint, *Codes*, In eds. R. L. Graham, M. Grötschel, and L. Lovász, *Handbook of Combinatorics*, vol. I, pp. 773–807. North-Holland, Amsterdam, New York, Oxford, (1995).

[10] J. H. van Lint, *Introduction to Coding Theory*. (Springer, Berlin, Heidelberg, New York, 1999), 3rd edition.

[11] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*. (MIT Press, Cambridge, 1972), 2nd edition.

[12] R. Roth, *Introduction to Coding Theory*. (Cambridge Univ. Press, Cambridge, 2006).

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. (North-Holland, Amsterdam, New York, Oxford, 1977; 12. impression 2006).

[14] T. M. Thompson, *From Error-Correcting Codes through Sphere Packings to Simple Groups*. (Carus Math. Monograph **21**, 1983).

[15] A. R. Calderbank, The art of signaling: fifty years of coding theory, *IEEE Trans. Inform. Theory*. **44**, 2561–2595, (1998).

[16] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.* **42**, 79–94, (1963).

[17] F. J. MacWilliams, N. J. A. Sloane, and J.-M. Goethals, The MacWilliams identities for non-linear codes, *Bell System Tech. J.* **51**, 803–819, (1972).

[18] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Reports Suppl.* **10**, (1973).

[19] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*. vol. I and II, *Encyclopedia of Math. and Its Applications* **69/78**, (Cambridge Univ. Press, Cambridge, 1999).

[20] P. J. Cameron, *Parallelisms of Complete Designs*. (Cambridge Univ. Press, Cambridge, 1976).

[21] C. J. Colbourn and J. H. Dinitz, Eds., *Handbook of Combinatorial Designs*. (CRC Press, Boca Raton, 2006), 2nd edition.

[22] M. Hall, Jr., *Combinatorial Theory*. (J. Wiley, New York, 1986), 2nd edition.

[23] D. R. Hughes and F. C. Piper, *Design Theory*. (Cambridge Univ. Press, Cambridge, 1985).

[24] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*. (Springer, Berlin, Heidelberg, New York, 2004).

[25] P. Dembowski, *Finite Geometries*. (Springer, Berlin, Heidelberg, New York, 1968; Reprint 1997).

[26] F. Buekenhout, Ed., *Handbook of Incidence Geometry*. (North-Holland, Amsterdam, New York, Oxford, 1995).

[27] P. J. Cameron, *Permutation Groups*. (Cambridge Univ. Press, Cambridge, 1999).

[28] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*. (Ginn, Boston, 1937; Reprint: Dover Publications, New York, 1956).

[29] J. D. Dixon and B. Mortimer, *Permutation Groups*. (Springer, Berlin, Heidelberg, New York, 1996).

[30] H. Wielandt, *Finite Permutation Groups*. (Academic Press, New York, 1964).

[31] V. D. Tonchev, *Combinatorial Configurations: Designs, Codes, Graphs*. (Longman, Harlow, 1988).

[32] D. Pei, *Authentication Codes and Combinatorial Designs*. (CRC Press, Boca Raton, 2006).

[33] D. R. Stinson, *Combinatorial designs and cryptography*, In ed. K. Walker, *Surveys in Combinatorics, 1993*, pp. 257–287. Cambridge Univ. Press, Cambridge, (1993).

[34] C. J. Colbourn, J. H. Dinitz, and D. R. Stinson, *Applications of combinatorial designs to communications, cryptography, and networking*, In eds. J. D. Lamb and D. A. Preece, *Surveys in Combinatorics, 1999*, pp. 37–100. Cambridge Univ. Press, Cambridge, (1999).

[35] P. Kaski and P. R. J. Östergård, *Classification Algorithms for Codes and Designs*. (Springer, Berlin, Heidelberg, New York, 2006).

[36] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*. (Cambridge Univ. Press, Cambridge, 1994; Reprint 1996).

[37] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*. (Cambridge Univ. Press, Cambridge, 2001), 2nd edition.

[38] H. J. Ryser, Ed., *Combinatorial Mathematics*. (Math. Assoc. Amer., Buffalo, NY, 1963).

[39] R. L. Graham, M. Grötschel, and L. Lovász, Eds., *Handbook of Combinatorics*. vol. I and II, (North-Holland, Amsterdam, New York, Oxford, 1995).

[40] J. Steiner, Combinatorische Aufgabe, *J. Reine Angew. Math.* **45**, 181–182, (1853).

[41] R. J. Wilson, The early history of block designs, *Rend. Sem. Mat. Messina Ser. II.* **9**, 267–276, (2003).

[42] Y. J. Ionin and M. S. Shrikhande, *Combinatorics of Symmetric Designs*. (Cambridge Univ. Press, Cambridge, 2006).

[43] R. H. Bruck and H. J. Ryser, The non-existence of certain finite projective planes, *Canad. J. Math.* **1**, 88–93, (1949).

[44] C. W. H. Lam, L. Thiel, and S. Swiercz, The non-existence of finite projective planes of order 10, *Canad. J. Math.* **41**, 1117–1123, (1989).

[45] A. Beutelspacher, *Projective Planes*, In ed. F. Buekenhout, *Handbook of Incidence Geometry*, pp. 101–136. North-Holland, Amsterdam, New York, Oxford, (1995).

[46] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*. (Clarendon Press, Oxford, 1998), 2nd edition.

[47] D. R. Hughes and F. C. Piper, *Projective Planes*. (Springer, Berlin, Heidelberg, New York, 1982), 2nd edition.

[48] H. Lüneburg, *Translation Planes*. (Springer, Berlin, Heidelberg, New York, 1980).

[49] G. Pickert, *Projektive Ebenen*. (Springer, Berlin, Heidelberg, New York, 1975), 2nd edition.

[50] E. Mathieu, Mémoire sur l'étude des fonctions de plusieurs quantitiés, *J. Math. Pures Appl.* **6**, 241–323, (1861).

[51] E. Mathieu, Sur la fonction cinq fois transitive de 24 quantités, *J. Math. Pures Appl.* **18**, 25–46, (1873).

[52] E. Witt, Die 5-fach transitiven Gruppen von Mathieu, *Abh. Math. Sem. Univ. Hamburg.* **12**, 256–264, (1938).

[53] E. Witt, Über Steinersche Systeme, *Abh. Math. Sem. Univ. Hamburg.* **12**, 265–275, (1938).

[54] H. Lüneburg, *Transitive Erweiterungen endlicher Permutationsgruppen.* (Springer, Berlin, Heidelberg, New York, 1969).

[55] M. Aschbacher, *Sporadic Groups.* (Cambridge Univ. Press, Cambridge, 1994).

[56] J. Tits, Sur les systèmes de Steiner associés aux trois "grands" groupes de Mathieu, *Rendic. Math.* **23**, 166–184, (1964).

[57] H. Lüneburg, Fahnenhomogene Quadrupelsysteme, *Math. Z.* **89**, 82–90, (1965).

[58] M. Huber, Classification of flag-transitive Steiner quadruple systems, *J. Combin. Theory, Series A.* **94**, 180–190, (2001).

[59] M. Huber, The classification of flag-transitive Steiner 3-designs, *Adv. Geom.* **5**, 195–221, (2005).

[60] M. Huber, The classification of flag-transitive Steiner 4-designs, *J. Algebr. Comb.* **26**, 183–207, (2007).

[61] M. Huber, A census of highly symmetric combinatorial designs, *J. Algebr. Comb.* **26**, 453–476, (2007).

[62] M. Huber, *Flag-transitive Steiner Designs.* (Birkhäuser, Basel, Berlin, Boston, to appear).

[63] L. Teirlinck, Non-trivial *t*-designs without repeated blocks exist for all *t*, *Discrete Math.* **65**, 301–311, (1987).

[64] R. A. Fisher, An examination of the different possible solutions of a problem in incomplete blocks, *Ann. Eugenics.* **10**, 52–75, (1940).

[65] E. F. Assmus, Jr. and H. F. Mattson, Jr., Coding and combinatorics, *SIAM Rev.* **16**, 349–388, (1974).

[66] E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes.* (Cambridge Univ. Press, Cambridge, 1993).

[67] E. F. Assmus, Jr. and J. D. Key, Designs and codes: an update, *Des. Codes Cryptography.* **9**, 7–27, (1996).

[68] I. F. Blake, Codes and designs, *Math. Mag.* **52**, 81–95, (1979).

[69] J. H. van Lint, *Codes and designs*, In ed. M. Aigner, *Higher Combinatorics: Proc. NATO Adv. Study Inst. (Berlin)*, pp. 241–256. Reidel, Dordrecht, Boston, (1977).

[70] J. H. van Lint, *Codes and combinatorial designs*, In eds. D. Jungnickel and S. A. Vanstone, *Proc. Marshall Hall conference on coding theory, design theory, group theory (Burlington, VT)*, pp. 31–39. J. Wiley, New York, (1993).

[71] V. D. Tonchev, *Codes and designs*, In eds. W. C. Huffman and V. Pless, *Handbook of Coding Theory*, vol. II, pp. 1229–1267. North-Holland, Amsterdam, New York, Oxford, (1998).

[72] V. D. Tonchev, *Codes*, In eds. C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, pp. 677–702. CRC Press, Boca Raton, 2nd edition, (2006).

[73] D. E. Muller, Application of boolean algebra to switching circuit design and to error correction, *IEEE Trans. Comp.* **3**, 6–12, (1954).

[74] I. S. Reed, A class of multiple-error-correcting codes and the decoding scheme, *IEEE Trans. Inform. Theory.* **4**, 38–49, (1954).

[75] E. F. Assmus, Jr. and H. F. Mattson, Jr., On tactical configurations and error-correcting codes, *J. Combin. Theory, Series A.* **2**, 243–257, (1967).

[76] M. J. E. Golay, Notes on digital coding, *Proc. IRE.* **37**, 657, (1949).

[77] V. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory, Series A.* **5**, 215–228, (1968).

[78] A. Tietäväinen, On the nonexistence of perfect codes over finite fields, *SIAM J. Appl. Math.* **24**, 88–96, (1973).

[79] J. H. van Lint, *Nonexistence theorems for perfect error correcting codes*, In eds. G. Birkhoff and M. Hall, Jr., *Computers in Algebraic Number Theory*, vol. IV, pp. 89–95. SIAM-AMS Proc., Providence, RI, (1971).

[80] V. A. Zinov'ev and V. K. Leont'ev, The nonexistence of perfect codes over Galois fields, *Probl. Control and Inform. Theory.* **2**, 123–132, (1973).

[81] M. R. Best. *A contribution to the nonexistence of perfect codes.* PhD thesis, University of Amsterdam, (1982).

[82] Y. Hong, On the nonexistence of unknown perfect 6- and 8-codes in Hamming schemes $H(n,q)$ with $q$ arbitrary, *Osaka J. Math.* **21**, 687–700, (1984).

[83] J. H. van Lint, A survey of perfect codes, *Rocky Mountain J. Math.* **5**, 189–224, (1975).

[84] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes.* (North-Holland, Amsterdam, New York, Oxford, 1997).

[85] A. M. Romanov, A survey of methods for constructing nonlinear perfect binary codes, *Diskretn. Anal. Issled. Oper. Ser. 1.* **13**, 60–88, (2006).

[86] S. V. Avgustinovich, O. Heden, and F. I. Solov'eva, The classification of some perfect codes, *Des. Codes Cryptography.* **31**, 313–318, (2004).

[87] O. Heden and M. Hessler, On the classification of perfect codes: side class structures, *Des. Codes Cryptography.* **40**, 319–333, (2006).

[88] K. T. Phelps, J. Rifà, and M. Villanueva, Kernels and $p$-kernels of $p^r$-ary 1-perfect codes, *Des. Codes Cryptography.* **37**, 243–261, (2005).

[89] P. Kaski, P. R. J. Östergård, and O. Pottonen, The Steiner quadruple systems of order 16, *J. Combin. Theory, Series A.* **113**, 1764–1770, (2006).

[90] P. R. J. Östergård and O. Pottonen, There exist Steiner triple systems of order 15 that do not occur in a perfect binary one-error-correcting code, *J. Combin. Des.* **15**, 465–468, (2007).

[91] J.-M. Goethals and S. Snover, Nearly perfect binary codes, *Discrete Math.* **2**, 65–88, (1972).

[92] N. V. Semakov, V. A. Zinov'ev, and G. V. Zaitsev, Uniformly packed codes, *Probl. Peredaci Inform.* **7**, 38–50, (1971).

[93] J.-M. Goethals and H. C. A. van Tilborg, Uniformly packed codes, *Philips Res. Reports.* **30**, 9–36, (1975).

[94] H. C. A. van Tilborg. *Uniformly packed codes.* PhD thesis, Technology University Eindhoven, (1976).

[95] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, On perfect codes and related concepts, *Des. Codes Cryptography.* **22**, 221–237, (2001).

[96] M. Schwartz and T. Etzion, Codes and anticodes in the Grassman graph, *J. Combin. Theory, Series A.* **97**, 27–42, (2002).

[97] V. Pless, The weight of the symmetry code for $p = 29$ and the 5-designs obtained therein, *Ann. New York Acad. Sci.* **175**, 310–313, (1970).

[98] V. Pless, Symmetry codes over $GF(3)$ and new five-designs, *J. Combin. Theory, Series A.* **12**, 119–142, (1972).

[99] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory, Series A.* **6**, 122–151, (1969).

[100] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward, Self-dual codes over $GF(4)$, *J. Combin. Theory, Series A.* **25**, 288–318, (1978).

[101] L. J. Paige, A note on the Mathieu groups, *Canad. J. Math.* **9**, 15–18, (1956).

[102] M. Harada, New 5-designs constructed from the lifted Golay code over $\mathbb{Z}_4$, *J. Com-*

*bin. Des.* **6**, 225–229, (1998).

[103] T. A. Gulliver and M. Harada, Extremal double circulant type II codes over $\mathbb{Z}_4$ and construction of 5-$(24, 10, 36)$ designs, *Discrete Math.* **194**, 129–137, (1999).

[104] A. Bonnecaze, P. Solé, and A. R. Calderbank, Quaternary quadratic residue codes and unimodular lattices, *IEEE Trans. Inform. Theory.* **41**, 366–377, (1995).

[105] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Information and Control.* **23**, 407–438, (1973).

[106] K. Tanabe, A criterion for designs in $\mathbb{Z}_4$-codes on the symmetrized weight enumerator, *Des. Codes Cryptography.* **30**, 169–185, (2003).

[107] A. R. Calderbank, P. Delsarte, and N. J. A. Sloane, A strengthening of the Assmus-Mattson theorem, *IEEE Trans. Inform. Theory.* **37**, 1261–1268, (1991).

[108] G. T. Kennedy and V. Pless, On designs and formally self-dual codes, *Des. Codes Cryptography.* **4**, 43–55, (1994).

[109] J. Simonis, MacWilliams identities and coordinate partitions, *Linear Algebra Appl.* **216**, 81–91, (1995).

[110] C. Bachoc, On harmonic weight enumerators of binary codes, *Des. Codes Cryptography.* **18**, 11–28, (1999).

[111] J.-L. Kim and V. Pless, Designs in additive codes over $GF(4)$, *Des. Codes Cryptography.* **30**, 187–199, (2003).

[112] D.-J. Shin, P. V. Kumar, and T. Helleseth, An Assmus-Mattson-type approach for identifying 3-designs from linear codes over $\mathbb{Z}_4$, *Des. Codes Cryptography.* **31**, 75–92, (2004).

[113] T. Britz and K. Shiromoto, Designs from subcode supports of linear codes, *Des. Codes Cryptography.* **46**, 175–189, (2008).

[114] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, On the existence of a projective plane of order 10, *J. Combin. Theory, Series A.* **14**, 66–78, (1973).

[115] C. W. H. Lam, The search for a finite projective plane of order 10, *Amer. Math. Monthly.* **98**, 305–318, (1991).

[116] P. J. Cameron, *Finite Geometries*, In eds. R. L. Graham, M. Grötschel, and L. Lovász, *Handbook of Combinatorics*, vol. I, pp. 647–692. North-Holland, Amsterdam, New York, Oxford, (1995).

[117] E. F. Assmus, Jr. and J. D. Key, *Polynomial codes and finite geometries*, In eds. W. C. Huffman and V. Pless, *Handbook of Coding Theory*, vol. II, pp. 1269–1343. North-Holland, Amsterdam, New York, Oxford, (1998).

[118] J. A. Thas, Finite geometries, varieties and codes, *Doc. Math. J. DMV,* Extra Vol. ICM III. pp. 397–408, (1998).

[119] L. Storme. Projective geometry and coding theory, COM$^2$MAC Lect. Note Series **9**. Combin. and Comput. Math., Center Pohang Univ. of Science and Technology, (2003).

[120] C. Hering. On codes and projective designs. Technical Report 344, Kyoto Univ., Math. Research Inst. Seminar Notes, (1979).

[121] P. J. Cameron. Finite geometry and coding theory, Socrates Course Notes, (1999). Published electronically at `http://dwispc8.vub.ac.be/Potenza/lectnotes.html`.

[122] T. Beth and D. Jungnickel, *Mathieu groups, Witt designs, and Golay codes*, In eds. M. Aigner and D. Jungnickel, *Geometries and Groups*, pp. 157–179. Springer, Berlin, Heidelberg, New York, (1981).

[123] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* (Springer, Berlin, Heidelberg, New York, 1998), 3rd edition.

[124] J. H. Conway and N. J. A. Sloane, Lexicographic codes: error-correcting codes from game theory, *IEEE Trans. Inform. Theory.* **32**, 337–348, (1986).

[125] R. T. Curtis, A new combinatorial approach to $M_{24}$, *Math. Proc. Cambridge Philos. Soc.* **79**, 25–42, (1976).

[126] E. F. Assmus, Jr. and H. F. Mattson, Jr., Perfect codes and the Mathieu groups, *Arch. Math.* **17**, 121–135, (1966).

[127] N. J. A. Sloane, The Sphere Packing Problem, *Doc. Math. J. DMV,* Extra Vol. ICM III. pp. 387–396, (1998).

[128] J. Leech, Some sphere packings in higher space, *Canad. J. Math.* **16**, 657–682, (1964).

[129] J. H. Conway and N. J. A. Sloane, Twenty-three constructions for the Leech lattice, *Proc. Roy. Soc. Lond., Series A.* **381**, 275–283, (1982).

[130] K. Schütte and B. L. van der Waerden, Das Problem der dreizehn Kugeln, *Math. Ann.* **125**, 325–334, (1953).

[131] P. Delsarte, Bounds for unrestricted codes, by linear programming, *Philips Res. Reports.* **27**, 272–289, (1972).

[132] P. Delsarte, J.-M. Goethals, and J. Seidel, Spherical codes and designs, *Geom. Dedicata.* **6**, 363–388, (1977).

[133] A. M. Odlyzko and N. J. A. Sloane, New bounds on the number of unit spheres that can touch a unit sphere in $n$ dimensions, *J. Combin. Theory, Series A.* **26**, 210–214, (1979).

[134] V. I. Levenshtein, On bounds for packings in $n$-dimensional Euclidean space, *Sov. Math. Doklady.* **20**, 417–421, (1979).

[135] O. R. Musin, The kissing number in four dimensions, *Ann. Math.* (to appear). Preprint published electronically at `http://arxiv.org/abs/math.MG/0309430`.

[136] H. Cohn and A. Kumar, The densest lattice in twenty-four dimensions, *Electron. Res. Announc. Amer. Math. Soc.* **10**, 58–67, (2004).

[137] H. Cohn and A. Kumar, Optimality and uniqueness of the Leech lattice among lattices, *Ann. Math.* (to appear). Preprint published electronically at `http://arxiv.org/abs/math.MG/0403263`.

[138] H. Cohn and N. D. Elkies, New upper bounds on sphere packings, *Ann. Math.* **157**, 689–714, (2003).

[139] O. R. Musin. An extension of Delsarte's method. The kissing problem in three and four dimensions. In *Proc. COE Workshop on Sphere Packings (Kyushu Univ. 2004)*, pp. 1–25, (2005).

[140] N. D. Elkies, Lattices, linear codes, and invariants, *Notices Amer. Math. Soc.* **47**, 1238–1245 and 1382–1391, (2000).

[141] F. Pfender and G. M. Ziegler, Kissing numbers, sphere packings and some unexpected proofs, *Notices Amer. Math. Soc.* **51**, 873–883, (2004).

[142] K. Bezdek, Sphere packings revisited, *Europ. J. Comb.* **27**, 864–883, (2006).

[143] G. Nebe and N. J. A. Sloane. A catalogue of lattices. Published electronically at `http://www.research.att.com/~njas/lattices/`.

[144] R. C. Bose and T. Shimamoto, Classification and analysis of partially balanced incomplete block designs with two associate classes, *J. Amer. Statist. Assoc.* **47**, 151–184, (1952).

[145] R. C. Bose and D. M. Mesner, On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Statist.* **30**, 21–38, (1959).

[146] E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes.* (Benjamin, New York, 1984).

[147] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs.* (Springer, Berlin, Heidelberg, New York, 1989).

[148] A. E. Brouwer and W. H. Haemers, *Association Schemes*, In eds. R. L. Graham,

M. Grötschel, and L. Lovász, *Handbook of Combinatorics*, vol. I, pp. 747–771. North-Holland, Amsterdam, New York, Oxford, (1995).

[149] P. Camion, *Codes and association schemes: Basic properties of association schemes relevant to coding*, In eds. W. C. Huffman and V. Pless, *Handbook of Coding Theory*, vol. II, pp. 1441–1567. North-Holland, Amsterdam, New York, Oxford, (1998).

[150] P. Delsarte and V. Levensthein, Association schemes and coding theory, *IEEE Trans. Inform. Theory.* **44**, 2477–2504, (1998).

[151] G. Nebe and N. J. A. Sloane. Table of the highest kissing numbers presently known. Published electronically at `http://www.research.att.com/∼njas/lattices/`.

[152] C. Bachoc and F. Vallentin, New upper bounds for kissing numbers from semidefinite programming. Preprint published electronically at `http://arxiv.org/abs/math.MG/0608426`.

# Index